IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

AI-Driven Solutions for Detecting and Mitigating Cyber Threats on Social Media Networks

Mani Gopalsamy
Senior Cyber Security Specialist, Louisville, KY, USA
manigopalsamy14@gmail.com

Abstract: *Cybersecurity has emerged as a vital aspect of organisations' operation because of the increased usage of technology and the internet, and an increase in callous and legal cybercrimes. Therefore, understanding and managing cyber threats has become an essential component of modern cyber architectures in order to provide protection and sustain technology assets and offerings against ever-involving cyber threats. The purpose of this article is to highlight the importance of vulnerability information analysis and cyberthreats in order to proactively comprehend cyber risks and anomalies and provide suitable mitigation techniques. The current research provides the prospect of an improved approach for responding to cyber threats on social media networks based on AI and machine learning. Leveraging the CIC-IDS2017 dataset. Data using text-based features, like user behaviour and network activity, are then preprocessed and feature-engineered, for instance, by means of one-hot encoding. Classification models such as LSTM, GNB, and LDA were used to group various cyber hazards, such as malware propagation, into distinct groups. Thus, the LSTM reveals its high potential in real-time threat identification in terms of an accuracy of 99.34%, recall of 99%, precision of 99.3%, and an F1-score of 99.34%. However, it reveals that GNB and LDA have lower accuracy and classification measures compared to other algorithms. In case of threat identification, the process of counteraction is also performative immediately as users are informed and accounts are blocked additionally to informing the admins. This framework provides a sound approach to improve the cybersecurity on social media websites.*

Keywords: Cyber security, Threat detection, mitigating threats, social networks, LSTM, machine learning

I. INTRODUCTION

Internet technology has developed very quickly to transform the manner people communicate, disseminate and unite at the global level. As social media gains more importance in day-to-day life, social platforms such as Facebook, Twitter, Instagram, and YouTube contain billions of active users[1]. Many of these platforms enable users to share messages, documents, photos, and videos and voice concerns and opinions [2]. In today's world, social media platforms are indispensable for personal, professional, and cultural contacts due to their widespread availability and ease of use. But at the same time, it raises magnificent levels of risks inclusive of cyber risks, especially those executing and using these connections to spread malware, phishing attempts, and other manifestations of cybercrime[3].

Threats within social media have, therefore, developed concurrently with the emergence of these platforms[4][5]. Ransomware, phishing, malware and social engineering continue to threaten ordinary users and organisationsjeopardising the security of data confidentiality, integrity as well as availability[6][7]. These threats may be engineered by nation-states, hackers or cyber criminals; their objectives may be spycraft, gain, politics, and mayhem[8]. Actual cyber threats include viruses, worms, Trojan horses, spyware, adware, phishing, pharming[9], DoS and DDoS, and identity thefts[10], all of them being breaches of the system or network[11]. Individuals, organisations, and occasionally physical infrastructure are at risk due to the dynamic nature of cyber threats, which evolve in tandem with technological advancements[12][13]. To mitigate these threats, then, some sophisticated security measures that can be used to detect, prevent and counter threats are needed[14][15].

It requires application of high-end machine learning as well as real-time analytics to identify, inhibit as well as counteract cyber threats in all the application domains [16][17]. AI can process hundreds of thousands of messages and signals at the same time[18], and identify patterns and discrepancies possible only if one denotes them as potentially

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

malicious – like malware, phishing, or DDoS probes. By using AI,[19]it can track the content of social media to watch for suspicious activity like malicious links or fake accounts and using machine learning[18], models are constantly changing to combat new threats[20]. There are also response capabilities that enable the AI to address threats at the moment to decrease the impact of the negative consequences, and this is the reason why contemporary cybersecurity cannot do without an AI [21].

Motivation and Contribution of Study

As more people sign up for the various social networking sites, these sites have become more vulnerable to hack attacks, including phishing, virus spreading, and social engineering attacks. These sites contain abuses of enormous amounts of information generated in the user community, so it becomes complex to track and counter such threats in real real-time manner. Traditional security strategies are usually too slow and adequately equipped to counter current types of attacks effectively. The motivation for this study stems from the urgent need to develop AI-driven solutions capable of proactively detecting and mitigating cyber threats on social media, thereby enhancing user safety and platform integrity. There are numerous contributions of this study that are multifaceted and impactful in the domain of cyber threat detection. Here's a detailed summary of the key contributions:

- Build an AI-driven framework for detecting and mitigating cyber threats on social media networks.
- Addresses class imbalances and improves detection accuracy using techniques like SMOTE.
- Utilizes advanced ML models like LDA, LSTM, and GNB to automatically identify threats.
- Provides a comprehensive evaluation of model performance employing standard metrics (e.g., F1-score, recall, accuracy, precision).

Structure of paper

This is how the rest of the paper is structured. Provide an overview of the literature on ML-based cyber threat detection on social networks in Section II. Section III presents methods and methodology, and Section IV results analysis and discussion. Section V presents the study's findings and future directions.

II. LITERATURE REVIEW

This section presents a selection of prior ML-based cybersecurity research. Some authors have tried to predict cyber-attacks on social media by using both ML and DL techniques. An use of cyber threat detection was discussed.

This paper Cheah and Chua, (2022) find ways to categorise hashtags according to their content, using relevant and irrelevant algorithms. This paper showcases two machine learning methods: one that uses a dictionary-based approach to predict how relevant hashtags will be to tweet content on an unlabeled dataset and another that uses supervised learning techniques like SVM, NBC, and DT algorithms to predict how relevant hashtags will be to tweet content and compares the machine's performance on labelled datasets.The SVM outperformed the other models in our relevance-hashtag classification experiment by a wide margin, with a 93.36% accuracy, 96.19% F1 score, and 97.22% ROC-AVC score. The study's results provide an automated methodology for hashtag hijacking identification that improves upon prior research by adjusting to new external threats and overcoming the shortcomings of earlier studies[22].

This research Agarwal, (2022) equipped with a novel approach to identifying and detecting cyber attacks on load forecast data from the electric grid. Two steps are involved. The first step involves creating a benchmark with the use of unsupervised ML using actual load data from the past. The second stage involves classifying cyber dangers with the use of supervised ML algorithms. Lastly, a new hybrid model is built using ensemble techniques. Using a publicly accessible dataset, the innovative method achieved a remarkable 97.25 percent accuracy [23].

This study Almasri, Snober and Al-Haija, (2022) propose an innovative approach that integrates ML's pattern recognition with the network's programmability features and architecture to strengthen defences against Port Scanning and DoS assaults.Feature selection using Anova and application of selected features to various ML models led to the development of an ML method. When it came to DoS attacks (86.9% accuracy) and probe attacks (93.5% accuracy), the NB model was the most effective [24].

In this study Tekin and Yilmaz, (2021) The cyber security data collected from Twitter was processed using DL algorithms. After classifying cyber threat information (DDoS, malware, ransomware, etc.) based on the tweets in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

the dataset, recursive neural networks are used. The research found that 88.64% of the time, determining the relevance of cyber threat information was successful, and that 89.49% of the time, correctly identifying the kind of threat intelligence was also successful [25].

In this paper, Singh, Mehtre and Sangeetha, (2019) have concentrated on a method of user behaviour profiling in order to track and examine the sequence of actions taken by users in order to identify potential insider threats. They provide an ML ensemble that uses CNN for time series anomaly detection and MSLSTM for spatial-temporal behaviour characteristics to identify additive outliers in behaviour patterns. It turns out that Multistate LSTM works better than the original, simpler LSTM. Once trained using the publicly available dataset for insider threats, the proposed technique using Multistate LSTM is able to identify these risks with an AUC of 0.9042 on train data and an AUC of 0.9047 on test data [26]. The following table 1 provides a comparative analysis of the background study based on its performance.

Table 1: Comparative analysis of previous work on cyber threats on social media

Reference	Data	Methodology	Results	Limitations/future work
Cheah & Chua (2022)	Unlabeled dataset of tweets	Dictionary-based unsupervised method and supervised methods (SVM, Naive Bayes, Decision Tree)	SVM achieved 93.36% accuracy, 96.19% F1 score, and 97.22% ROC-AUC score.	Limited to hashtag relevance; may not generalise to other text types. Future work could explore other social media data and classification methods.
Agarwal (2022)	Historical electric grid load data	Two-stage methodology: unsupervised learning for benchmarking and supervised learning for threat categorisation; hybrid ensemble model	Achieved 97.25% accuracy using a hybrid model on publicly available datasets.	Focused on electric grid data, results may not apply to other sectors. Future work could extend the methodology to critical infrastructures beyond the electric grid.
Almasri et al. (2022)	Network traffic data	Machine learning pattern recognition and feature selection using ANOVA	Naive Bayes achieved 86.9% accuracy for DoS attacks and 93.5% for Probe attacks.	Focused on specific attack types; generalizability to other threats not assessed. Future research could evaluate performance against a wider variety of cyber threats.
Tekin& Yilmaz (2021)	Twitter data related to cyber threat intelligence	Deep learning models using recursive neural networks for threat classification	88.64% accuracy for relevance detection and 89.49% for threat type classification.	Limited to tweets; may not consider other relevant data sources. Future work could incorporate data from additional social media platforms for improved classification.
Singh et al. (2019)	Publicly available dataset for insider threats	Ensemble hybrid approach using Multi-State LSTM and CNN for time series anomaly detection	Achieved AUC of 0.9042 on training data and 0.9047 on test data for insider threat detection.	Computationally intensive; relies on specific features which may require large datasets. Future work could refine feature selection methods and explore different insider threat types.

III. METHODOLOGY

In order to detect and mitigate cyber risks on social media networks, a technique based on AI must be implemented effe ct. The first step in identifying possible cyber risks is collecting the CIC-IDS2017 dataset. Figure 1 shows the flow of data in various steps and phases. The data is then cleaned during preprocessing by eliminating unnecessary information, duplicates, and missing values. The next step is featuring engineering, which takes the unstructured data and makes it suitable for machine learning by adding text-based features like keywords, patterns of user behaviour, and network activity. To make text data more amenable to machine learning models, methods such as one-hot encoding can be used to transform it into numerical representations. By oversampling minority groups that represent cyber dangers, techniques like SMOTE can help correct class inequalities. Next, the system uses LDA, LSTM or GNB, which are deep

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

learning models, to identify different kinds of threats, such as malware transmission or threat. A confusion matrix, together with metrics like recall, accuracy, precision, and F1-score, is used to assess a model's classification performance. Automatic mitigation measures are activated upon threat detection. These strategies may involve alerting users, banning or stating criminal accounts, or informing platform administrators to take further action.

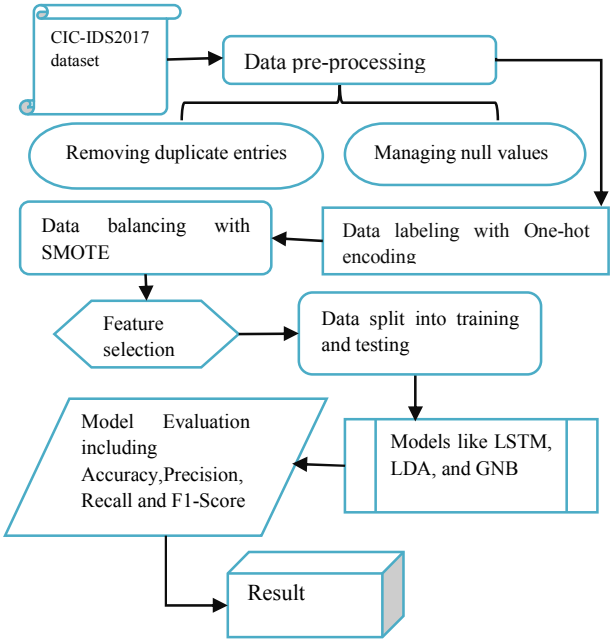

Figure 1: dataflow diagram for mitigating cyber threats on social media

Detailed explanations of each step in creating a data flow diagram are provided below.

A. Data collection

IDSs rely on representative network datasets like the CIC-IDS2017 dataset, and benchmark datasets serve as the foundation for comparing various IDSs. One modern dataset on network intrusions is this one, which is based on flow analysis. In 2016, a set of eleven criteria was released that outlined the necessary characteristics for an accurate intrusion detection dataset. CICIDS2017 is a novel and exhaustive dataset because it meets all of these requirements.The visualization and analysis of the dataset are provided below:

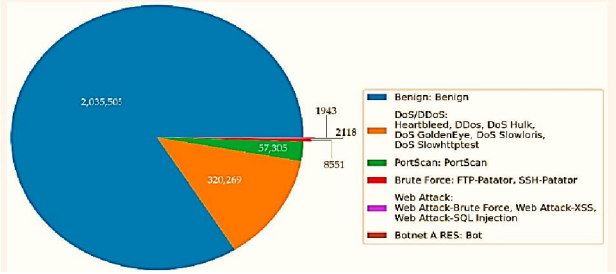

Figure 2: Class distribution of the original CICIDS2017

The following figure 2 shows the class distribution of data. A CICIDS2017 dataset contains 2,035,505 benign instances and several attack types with imbalances. DoS/DDoS accounts for 57,305 instances, PortScan for 320,269, Brute Force for 8,551, Web Attacks (Brute Force, XSS, SQL Injection) for 2,118, and Botnet for 1,943. This distribution is key for analyzing and improving intrusion detection systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

B. Data Processing

The dataset has to be pre-processed before the experiment could begin. The first step was to clean the dataset by removing any unnecessary entries.Due of their little contribution to the dataset, items with missing or infinite values were excluded. For the models to be exposed to as many distinct examples as feasible, we also eliminated duplicates. Further preprocessing key terms are as follow:

C. One-hot encoding for labelling

The process of transforming categorical data into a numerical representation that ML models can use is known as data encoding. For nominal categorical data, one-hot encoding is essentially a feature engineering technique. Data must be transformed into numerical form in order to apply ML to categorical data without the need for a tree-based approach.

D. Data balancing with SMOTE

Randomly increasing the sample size is the quickest approach to boost the minority class size, but it might lead to overfitting. SMOTE, or synthetic minority oversampling, is a method for using KNN to inject duplicate instances into the training set in order to decrease the likelihood of overfitting[27]. Equation (1) is used by SMOTE.

$$x_{syn} = x_i + (k_{nn} - x_i)xt \ldots . (1)$$

Which xi for a feature vector, known for the KNN and t for a random number from 0 to 1.

E. Feature Selection

Feature selection consists of determining the most impactful features for a problem. The performance-enhancing aspects of feature selection make it a popular tool for identifying the most relevant features[28]. This requires in-depth knowledge of the data being used to determine which features should be included.

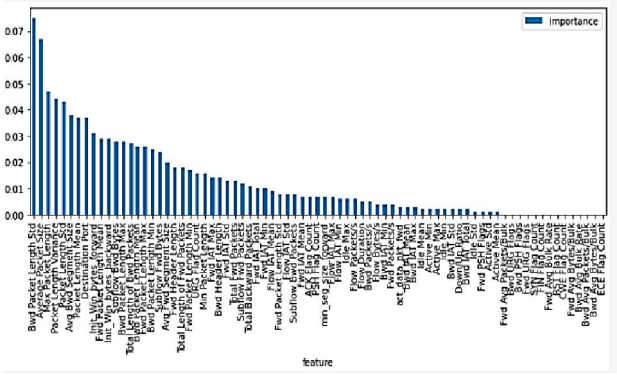

Figure 3: Importance score of each feature in CIC-IDS2017 dataset

The CIC-IDS2017 dataset's importance scores for each characteristic are shown in Figure 3, a bar graph. It highlights a significance of various features within a dataset, with the importance scores ranging from 0.00 to 0.07. With greater significance scores, the characteristics on the left side of the graph are more significant within the context of the dataset.

F. Data splitting

To train and test models, it is necessary to divide the data into separate sets, a process known as data splitting. There are two sets of data used in this research: the training set and the testing set. Seventy percent of the data is in the training data, whereas thirty percent is in the testing data. The ratio of data splitting is 70:30.

G. Classification with LSTM model

This thesis makes use of LSTM, the most popular deep-learning approach currently available[29]. A recurrent neural network design used in DL, it is artificial. In contrast to traditional feed-forward neural networks, LSTM models include feedback linkages[30]. It is capable of processing whole data sequences as well as particular data points. While

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

LSTMs do have a chainlike structure, their repeating modules are unique[31]. Figure 4 shows that instead of the usual neural network layers, they use "cell blocks," which include components like input gates, forget gates, and output gates.

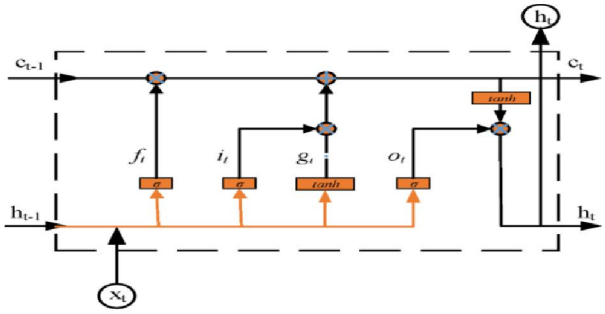

Figure 4: Diagram of LSTM cell

The inputs to the LSTM include the output from the previous time step (h t → 1) and the current time step (xt), which are used by the memory cells to find out what data was erased by the forget gate. According to (2), the forget gate ft guides the deletion of specific pieces of data from earlier memory cells:

$$f_t = \sigma\left(w_{fx}x_t + w_{fh}h_{t-1} + b_f\right) \dots\dots\dots (2)$$

The sigmoid function is denoted by σ, the weights w fx and w fh at time t represent the input layer to the forget gate's hidden layer and the preceding hidden layer to the forget gate's hidden layer, respectively, and b f represents the forget gate's bias. After then, it is necessary for the memory cells to ascertain the current state ct − 1, the input gate it, the candidate value gt, the forget gate ft, and the updated new information. The procedure by which the memory cells ascertain the revised data may be defined using the following formula.

$$i_t = \sigma(w_{ix}x_t + w_{ih}h_{t-1} + b_i) \dots\dots\dots (3)$$

$$g_t = \sigma\left(w_{gx}x_t + w_{gh}h_{t-1} + b_g\right) \dots\dots\dots (4)$$

$$c_t = f_t \otimes c_{t-1} + i_t \otimes g_t \dots\dots\dots (5)$$

where w ix and w ih represent the weight of the input layer to the input gate's hidden layer and the weight of the previous hidden layer to the input gate's hidden layer at time t, respectively; b i and b g represent the input gate's and the candidate gate's biases, respectively; c t represents the current cell state; tanh (·) denotes a hyperbolic tangent function; and ⊗ denotes element-wise multiplication. Lastly, the network determines the output in the memory cells based on the current state c t and the output gate ot, which is specified as (6):

$$o_t = \sigma(w_{ox}x_t + w_{oh}h_{t-1} + b_o) \dots\dots\dots (7)$$

$$h_t = o_t \otimes \tanh(c_t) \dots\dots\dots (8)$$

where bo is the output gate's bias, and wox and woh stand for the weight of the input layer to the output gate's hidden layer and the weight of the preceding hidden layer to the output gate's hidden layer at time t, respectively.

H. Performance matrix

It is necessary to understand how each metric is measured to select the evaluation metric to better assess the model. Classification accuracy was quantitatively expressed using a confusion matrix. Information on the actual and anticipated classes acquired by a classification system is included in the confusion matrix, which is one of the most used machine learning approaches. Predicted classes and actual classes are the two sides of the confusion matrix. The anticipated class state is shown in each column, whereas each row comprises an actual class example. True positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) are the four columns of the confusion matrix. The following matrix is explained in below:

Accuracy

Accuracy is the proportion of cases the model correctly categorised and the total error in class prediction. This measure summarises the model's performance across classes. However, skewed data may misrepresent performance. A classifier that mostly predicts the majority class may be accurate yet misclassify minority class occurrences. The formula of accuracy is (9):

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

$$Acuracy = \frac{TP + TN}{TP + TN + FN + FP} \ldots . (9)$$

Precision

The precision measures the accuracy of the positive data predictions. A lower number of false positives is an indication of high precision. The formula of precision is (10):

$$Precision = \frac{TP}{TP + FP} \ldots . (10)$$

Recall

The recall is a statistic used to determine the completeness of the classifier. Higher recall means fewer false negatives, while poorer recall indicates more false negatives. Precision generally diminishes as recollection improves. Following formula of (11):

$$Recall = \frac{TP}{TP + FN} \ldots . (11)$$

F1-score

The F1-score or F-measure is the weighted harmonic mean of precision and recall. When the dataset is heavily imbalanced, this measure is the most appropriate to use. The equation (12) of f1-score is:

$$F1 - score = 2 * \frac{precision * recall}{precision + recall} \ldots . (12)$$

The following matrices are utilized to evaluate the model performance.

IV. RESULTS & DISCUSSIONS

A simulated results of cyber threat detection prediction based on ML techniques in mitigating cyber threats on social media networks discussed in this section. Results description across performance matrix like f1-score, recall, accuracy, and precision. A following table 2 provides the LSTM model performance for cyber threat detection using ML techniques.

Table 2: LSTM Model Performance on the CIC-IDS2017 dataset

Matrix	LSTM
Accuracy	99.34
Precision	99
Recall	99.3
F1-score	99.34

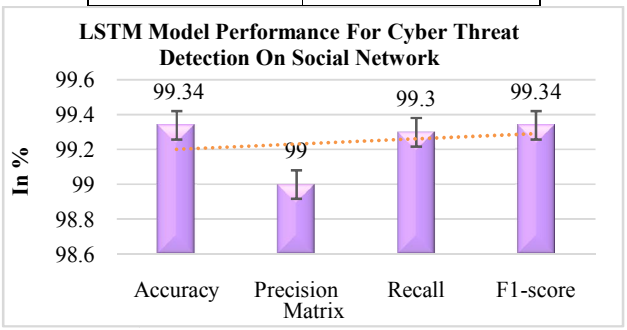

Figure 5: LSTM Performance for cyber threat detection on CICIDS2017 dataset

The above Table 2 and Figure5 shows the LSTM Performance. In this figure, LSTM model shows exceptional performance with 99.34% accuracy, 99% precision, 99.3% recall, and a 99.34% F1-score, indicating a highly effective and balanced classification capability.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

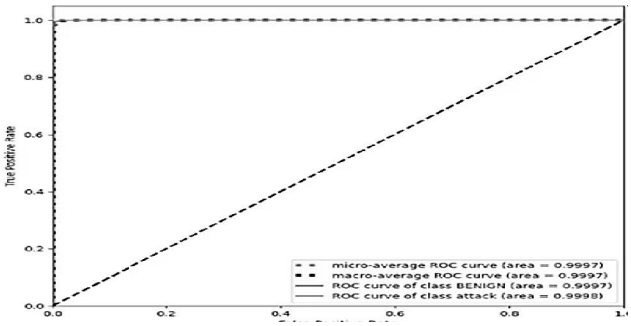

Figure 6: ROC curve for LSTM Model

The ROC curve in Figure6 for the LSTM model demonstrates outstanding performance in distinguishing between the 'BENIGN' and 'attack' classes. Both the micro-average and macro-average ROC curves have an AUC of 0.9997, while the AUC for the attack class is slightly higher at 0.9998. These near-perfect AUC values indicate the LSTM model's excellent ability to predict TP while minimising false positives, making it highly effective in detecting and classifying cyber threats with exceptional precision.

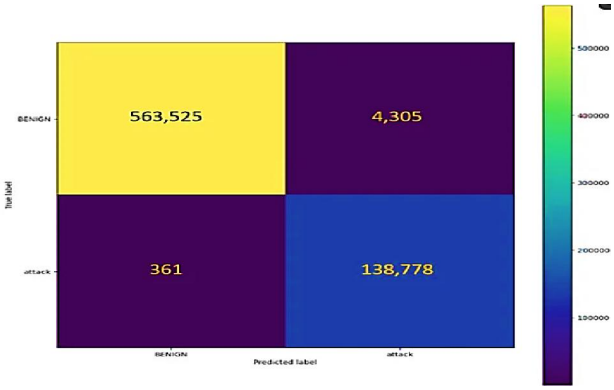

Figure 7: Confusion matrix for LSTM Model.

Figure 7's confusion matrix for the LSTM model demonstrates how well it performs in identifying assaults and benign acts. It correctly identified 563,525 benign cases (TP) and 138,778 attack cases (TN). However, 4,305 benign cases were misclassified as attacks (FN), and 361 attack cases were incorrectly labelled as benign (FP). Despite a few misclassifications, the model demonstrates high accuracy, with minimal errors, highlighting its effectiveness in distinguishing between benign and attack instances.

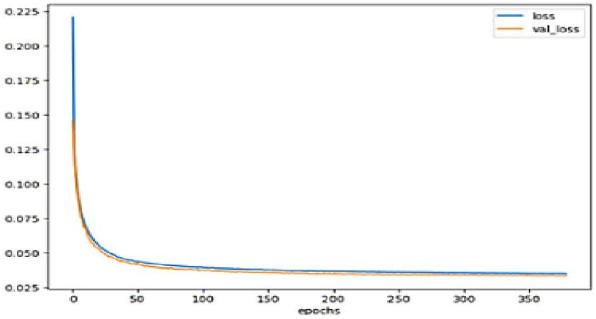

Figure 8: Loss curves for LSTM during the training process

Loss curves for LSTM during the training process in Figure 8show a typical pattern for neural network training, where both the training and validation loss decrease sharply in the early epochs, indicating rapid learning by the LSTM model. As training progresses over approximately 350 epochs, the curves level off, suggesting that the model's improvements slow down, with minimal gains in performance. This indicates that the model is approaching convergence, where further training yields only marginal benefits.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

Table 3: Comparison of model's performance for cyber threat detection

Models	LSTM	GNB[32]	LDA[33]
Accuracy	99.34	54.21	88.10
Recall	99	45.78	98.33
Precision	99.3	76.96	81.63
F1- score	99.34	53.68	89.21

The performance of the models are provided in Table 3 above. When comparing the performance of the LSTM, GNB, and LDA models for mitigating cyber threats, the LSTM model clearly outperforms the others. LSTM achieves an outstanding accuracy of 99.34%, with a high recall of 99%, precision of 99.3%, and F1-score of 99.34%, making it highly reliable in both detecting and accurately classifying cyber threats. In contrast, GNB shows poor performance with only 54.21% accuracy, a recall of 45.78%, and a relatively low F1-score of 53.68%, indicating it struggles with both precision and recall. LDA performs better than GNB, with an accuracy of 88.10%, recall of 98.33%, and an F1-score of 89.21%, but its precision of 81.63% suggests some limitations in accurately identifying true threats. Overall, LSTM proves to be the most effective model for mitigating cyber threats due to its superior accuracy and balance across key metrics.

V. CONCLUSION & FUTURE WORK

Cybersecurity is an important issue for many different kinds of businesses. There are software and design risks associated with system security. Predicting software assets' and processes' security vulnerabilities and implementing appropriate mitigation strategies are all part of the process. A plethora of approaches have been established, and the security requirements of software assets and processes have been defined. When designing software systems, threat modelling is a useful tool for identifying and meeting security needs.This research lays the groundwork for a strong AI-powered system to identify and counteract cyber-attacks on social media platforms. The ML approach effectively leverages machine learning techniques, specifically LSTM, to achieve high accuracy rates 99.34% in threat detection, significantly outperforming traditional models such as GNB and LDA. The results emphasise the use of modern mathematical statistics for real-time identification and reduction of threats, as well as the strengthening of the defences of social networks. However, there are limitations to the current study, even though positive results have been identified. The preoccupation with implicit threats detected with the help of the CIC-IDS2017 dataset may not contain the spectrum of the observed threats from different social media platforms. Further, the evaluation metrics are derived from a controlled environment which does not capture the real-world conditions adequately well. Further research should be directed towards expanding the dataset with the representation of many cyber risks and a variety of user engagements of them.

REFERENCES

[1] M. Gopalsamy, "Artificial Intelligence (AI) Based Internet-ofThings (IoT)-Botnet Attacks Identification Techniques to Enhance Cyber security," *Int. J. Res. Anal. Rev.*, vol. 7, no. 4, pp. 414–420, 2020, [Online]. Available: https://www.ijrar.org/papers/IJRAR2AA1742.pdf

[2] Mani Gopalsamy, "An Optimal Artificial Intelligence (AI) technique for cybersecurity threat detection in IoT Networks," *Int. J. Sci. Res. Arch.*, vol. 7, no. 2, pp. 661–671, Dec. 2022, doi: 10.30574/ijsra.2022.7.2.0235.

[3] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*. 2018. doi: 10.1093/cybsec/tyy006.

[4] A. M. Algarni, V. Thayananthan, and Y. K. Malaiya, "Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems," *Appl. Sci.*, 2021, doi: 10.3390/app11083678.

[5] M. Gopalsamy, "Advanced Cybersecurity in Cloud Via Employing AI Techniques for Effective Intrusion Detection," *Int. J. Res. Anal. Rev.*, vol. 8, no. 1, pp. 187–193, 2021, [Online]. Available: https://www.ijrar.org/papers/IJRAR21A1737.pdf

[6] Mani Gopalsamy, "A review on blockchain impact on in cybersecurity: Current applications, challenges and future trends," *Int. J. Sci. Res. Arch.*, vol. 6, no. 2, pp. 325–335, Aug. 2022, doi: 10.30574/ijsra.2022.6.2.0146.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

[7] M. S. Rajeev Arora, "Applications of Cloud Based ERP Application and how to address Security and Data Privacy Issues in Cloud application," *Himal. Univ.*, 2022.
[8] R. Arora, S. Gera, and M. Saxena, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 458–463.
[9] H. S. Chandu, "A Survey of Memory Controller Architectures: Design Trends and Performance Trade-offs," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 930–936, 2022, [Online]. Available: https://www.ijrar.org/papers/IJRAR22D3204.pdf
[10] K. Patel, "Quality Assurance In The Age Of Data Analytics: Innovations And Challenges," *Int. J. Creat. Res. Thoughts*, vol. 9, no. 12, pp. f573–f578, 2021.
[11] B. P. Poudel, A. Mustafa, A. Bidram, and H. Modares, "Detection and mitigation of cyber-threats in the DC microgrid distributed control system," *Int. J. Electr. Power Energy Syst.*, 2020, doi: 10.1016/j.ijepes.2020.105968.
[12] M. Gopalsamy, "Scalable Anomaly Detection Frameworks for Network Traffic Analysis in cybersecurity using Machine Learning Approaches," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 06, pp. 549–558, 2022.
[13] R. Bishukarma, "Adaptive AI-Based Anomaly Detection Framework for SaaS Platform Security," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 07, pp. 541–548, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.8.
[14] M. R. S. and P. K. Vishwakarma, "An Efficient Machine Learning Based Solutions for Renewable Energy System," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 951–958, 2022, [Online]. Available: https://www.ijrar.org/papers/IJRAR22D3208.pdf
[15] S. Pandey, "Transforming Performance Management Through Ai: Advanced Feedback Mechanisms, Predictive Analytics, And Bias Mitigation In The Age Of Workforce Optimization," *Int. J. Bus. Quant. Econ. Appl. Manag. reseacrh*, vol. 6, no. 7, pp. 1–10, 2020.
[16] A. Parlakkılıç, "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach," 2018.
[17] Mani Gopalsamy, "Enhanced Cybersecurity for Network Intrusion Detection System Based Artificial Intelligence (AI) Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 12, no. 01, pp. 671–681, Dec. 2021, doi: 10.48175/IJARSCT-2269M.
[18] J. Thomas, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.
[19] P. Khare, "The Impact ofAI on Product Management:A Systematic Review and Future Trends," *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 736–741, 2022.
[20] A. P. A. Singh, "Strategic Approaches To Materials Data Collection And Inventory Management," *Int. J. Bus. Quant. Econ. Appl. Manag. Res.*, vol. 7, no. 5, 2022.
[21] S. Pandey, "The Future of Recruitment: Analyzing the Impact of Artificial Intelligence on Evolving Hiring Processes and Strategies," *North Am. J. Eng. Res.*, vol. 3, no. 1, pp. 1–8, 2022, [Online]. Available: https://najer.org/najer/article/view/72/79
[22] W. L. Cheah and H. N. Chua, "Detection of Social Media Hashtag Hijacking Using Dictionary-based and Machine Learning Methods," in *4th IEEE International Conference on Artificial Intelligence in Engineering and Technology, IICAIET 2022*, 2022. doi: 10.1109/IICAIET55139.2022.9936788.
[23] A. Agarwal, "Load forecast anomaly detection under cyber attacks using a novel approach," in *Proceedings of 4th International Conference on Cybernetics, Cognition and Machine Learning Applications, ICCCMLA 2022*, 2022. doi: 10.1109/ICCCMLA56841.2022.9988990.
[24] T. Almasri, M. A. Snober, and Q. A. Al-Haija, "IDPS-SDN-ML: An Intrusion Detection and Prevention System Using Software-Defined Networks and Machine Learning," in *APICS 2022 - 2022 1st International Conference on Smart Technology, Applied Informatics, and Engineering, Proceedings*, 2022. doi: 10.1109/APICS56469.2022.9918804.
[25] U. Tekin and E. N. Yilmaz, "Obtaining Cyber Threat Intelligence Data from Twitter with Deep Learning Methods," in *ISMSIT 2021 - 5th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings*, 2021. doi: 10.1109/ISMSIT52890.2021.9604715.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, September 2023

[26] M. Singh, B. M. Mehtre, and S. Sangeetha, "User Behavior Profiling using Ensemble Approach for Insider Threat Detection," in *ISBA 2019 - 5th IEEE International Conference on Identity, Security and Behavior Analysis*, 2019. doi: 10.1109/ISBA.2019.8778466.

[27] S. Mishra, "Handling Imbalanced Data : SMOTE vs . Random Undersampling"," vol. 04, 2017.

[28] X. Deng, Y. Li, J. Weng, and J. Zhang, "Feature selection for text classification: A review," *Multimed. Tools Appl.*, 2019, doi: 10.1007/s11042-018-6083-5.

[29] P. Khare and I. Researcher, "Signature-Based Biometric Authentication: A Deep Dive Into Deep Learning Approaches," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 4, no. 8, Aug. 2022, doi: 10.56726/IRJMETS29522.

[30] S. Bauskar, "Business Analytics in Enterprise System Based on Application of Artificial Intelligence," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 04, no. 01, pp. 2582–5208, 2022, doi: 10.56726/IRJMETS18127.

[31] A. Sherstinsky, "Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network," *Phys. D Nonlinear Phenom.*, 2020, doi: 10.1016/j.physd.2019.132306.

[32] N. Meemongkolkiat and V. Suttichaya, "Analysis on Network Traffic Features for Designing Machine Learning based IDS," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1993/1/012029.

[33] A. Rosay, E. Cheval, F. Carlier, and P. Leroux, "Network Intrusion Detection: A Comprehensive Analysis of CIC-IDS2017," in *International Conference on Information Systems Security and Privacy*, 2022. doi: 10.5220/0010774000003120.